ACTA ARITHMETICA
131.2 (2008)

Résultants cycliques et polynômes cyclotomiques

par

Jean-Paul Bézivin (Caen)

1. Introduction et résultats. Dans cet article, nous allons revenir sur un sujet introduit par D. Fried dans [1], qui est celui des résultants cycliques.

Soit K un corps commutatif de caractéristique nulle, que l'on peut supposer algébriquement clos, et $P(X) = a_0 \prod_{i=1}^{d}(X-\lambda_i)$ un polynôme non nul à coefficients dans K. On note $r_n(P)$ le résultant de P et de X^n-1 pour $n \geq 1$:

$$r_n(P) = \mathrm{Res}(P, X^n - 1).$$

On appelle cette suite la suite des *résultants cycliques* de P.

On a immédiatement la formule $r_n(P) = a_0^n \prod_{i=1}^{d}(\lambda_i^n - 1)$. Dans toute la suite, on va supposer que les polynômes considérés n'ont pas de racines qui soient des racines de l'unité.

Le problème posé est de savoir dans quelle mesure la donnée des $r_n(P)$ pour $n \geq 1$ caractérise le polynôme P. Dans [1], D. Fried donne une réponse partielle à cette question dans le cas de polynômes réciproques à coefficients réels. Dans [2], C. J. Hillar reprend la question, et démontre le résultat général suivant :

Théorème 1.1 (C. Hillar). *Soient f et g deux polynômes de $\mathbb{C}[x]$ n'ayant pas comme zéros de racines de l'unité. Alors f et g engendrent la même suite de résultants cycliques si et seulement si il existe $u, v \in \mathbb{C}[x]$ avec $u(0) \neq 0$ et des entiers naturels l_1, l_2 tels que* $\deg(u) \equiv l_2 - l_1 \pmod 2$ *et*

$$f(x) = (-1)^{l_2-l_1} x^{l_1} v(x) u(x^{-1}) x^{\deg(u)}, \qquad g(x) = x^{l_2} v(x) u(x).$$

Nous renvoyons le lecteur à [3] pour d'autres renseignements sur l'utilisation de ces résultats dans divers domaines.

Nous utiliserons la dénomination introduite par C. Hillar : un polynôme $P(x) = \prod_{i=1}^{d}(X-\lambda_i)$ sera dit *générique* si les λ_i ne sont pas des racines de l'unité, et si la condition suivante est satisfaite. Notons pour S partie de

2000 *Mathematics Subject Classification*: Primary 11B83, 11B37; Secondary 12D05.
Key words and phrases: cyclic resultant, cyclotomic polynomial.

$\{1, \ldots, d\}$ par λ_S le produit $\prod_{i \in S} \lambda_i$, avec la convention que si S est vide, $\lambda_S = 1$. On demande alors que pour S et T parties distinctes de $\{1, \ldots, d\}$, on ait $\lambda_S \neq \lambda_T$.

Dans le cas particulier où l'on suppose que les deux polynômes f et g sont unitaires et génériques, il résulte du théorème de Hillar que si $r_n(f) = r_n(g)$ pour tout $n \geq 1$, alors $f = g$.

Il est alors naturel de se poser la question de savoir si un nombre fini d'égalités $r_n(f) = r_n(g)$ impliquent dans le cas générique que $f = g$, et de savoir (si une telle propriété est vraie) quel nombre de résultants cycliques égaux sont nécessaires pour avoir l'égalité $f = g$.

Dans [3], C. Hillar et L. Levine énoncent dans ce cas particulier la conjecture suivante :

CONJECTURE 1.2. *Un polynôme unitaire générique de degré d est déterminé par ses $d+1$ premiers résultants cycliques.*

Dans cet article, nous allons donner une réponse partielle à cette question :

THÉORÈME 1.3. *Soit d un entier ≥ 1. Il existe un ouvert de Zariski U de $\mathbb{C}^d$ tel que, si deux polynômes $P(X) = \prod_{k=1}^{d}(X - x_k)$ et $Q(X) = \prod_{k=1}^{d}(X - y_k)$ sont tels que $x = (x_1, \ldots, x_d)$ et $y = (y_1, \ldots, y_d)$ soient dans U et qu'aucune des composantes x_k ou y_k de x et y ne soit une racine de l'unité d'ordre $\leq d+1$, et si de plus $r_n(P) = r_n(Q)$ pour $1 \leq n \leq d+1$, alors $P = Q$.*

Cependant, notre méthode de démonstration de ce résultat ne nous permet pas de déterminer explicitement l'ouvert U, et en particulier de savoir si ce résultat s'applique à tout couple de polynômes unitaires génériques.

2. Réduction du problème. Pour $j \geq 1$, on note ϕ_j le j-ième polynôme cyclotomique ; son degré est donc $\varphi(j)$, où nous avons noté φ l'indicateur d'Euler. Soit $d \geq 1$. On a le premier résultat immédiat suivant :

PROPOSITION 2.1. *Soit N un entier naturel non nul, et $P(X) = \prod_{k=1}^{d}(X - x_k)$ un polynôme unitaire de degré $d \geq 1$ à coefficients dans $\mathbb{C}$, n'ayant aucune racine qui soit nulle ou une racine de l'unité d'ordre $\leq N$. Alors la donnée de $r_n(P) = \prod_{k=1}^{d}(x_k^n - 1)$ pour $1 \leq n \leq N$ équivaut à la donnée des $\prod_{k=1}^{d} \phi_j(x_k)$, $j = 1, \ldots, N$.*

Démonstration. Cela vient de la formule $X^n - 1 = \prod_{j|n} \phi_j(X)$, qui conduit à

$$r_n(P) = \prod_{j|n} \prod_{k=1}^{d} \phi_j(x_k),$$

et du fait que pour tout $h \leq N$ la quantité $\prod_{k=1}^{n} \phi_h(x_k)$ est non nulle. ∎

Du fait de ce résultat, la conjecture 1.2 devient :

CONJECTURE 2.2. *Soient* $P(X) = \prod_{k=1}^{d}(X-x_k)$, $Q(X) = \prod_{k=1}^{d}(X-y_k)$ *deux polynômes unitaires génériques de degré* d *à coefficients dans* $\mathbb{C}$. *Si* $\prod_{k=1}^{d}\phi_j(x_k) = \prod_{k=1}^{d}\phi_j(y_k)$ *pour* $1 \leq j \leq d+1$, *alors* $P = Q$.

En raison de cette forme de la conjecture, nous allons essentiellement travailler avec des polynômes cyclotomiques dans le reste de l'article.

3. Lemmes préliminaires. Nous allons commencer par rappeler des résultats d'A. Płoski ([4]). Soient n un entier, et $F = (F_1, \ldots, F_{n+1})$ une application polynomiale de $\mathbb{C}^n$ dans $\mathbb{C}^{n+1}$.

On dira que la famille $\{F_1, \ldots, F_{n+1}\}$ est *non dégénérée* si elle contient n éléments algébriquement indépendants sur $\mathbb{C}$.

Dans ce cas, l'extension $\mathbb{C}(F_1, \ldots, F_{n+1}) \subset \mathbb{C}(Z_1, \ldots, Z_n)$ est une extension algébrique finie. On note $q(F)$ son degré. Il existe, à un facteur multiplicatif non nul près, un unique polynôme P de degré minimal, irréductible, tel que $P(F_1, \ldots, F_{n+1}) = 0$.

On note de plus F_i^+ la partie homogène de plus haut degré du polynôme F_i.

On a le premier résultat suivant :

THÉORÈME 3.1 (A. Płoski). *Soit* $F = (F_1, \ldots, F_{n+1})$ *une application polynomiale non dégénérée,* $q = q(F)$ *et* P *comme définis ci-dessus. Alors on a*

$$\deg(P^q) \leq \max_{1\leq j\leq n+1}\Big\{\prod_{i\neq j}\deg(F_i)\Big\}. \tag{1}$$

Soit de plus i_0 *un indice tel que* $\deg(F_i) \geq \deg(F_{i_0})$ *pour tout* i. *Si le système d'équations* $F_i^+ = 0$, $i \neq i_0$, *n'a que la solution triviale nulle, alors l'inégalité* (1) *est une égalité.*

Démonstration. Voir [4, Theorem 1.1]. ∎

Soit $d \geq 1$. On note $\sigma_{k,d}(X_1, \ldots, X_d) = \sigma_{j,d}(X)$ le k-ième polynôme symétrique élémentaire en d variables, et on définit des polynômes symétriques $T_{j,d}$ de la façon suivante :

$$T_{j,d}(X) = T_{j,d}(X_1, \ldots, X_d) = \prod_{k=1}^{d}\phi_j(X_k).$$

Nous notons $Q_{j,d}$ l'unique polynôme en $Y_1, \ldots, Y_d$ tel que l'on ait $T_{j,d}(X) = Q_{j,d}(\sigma_{1,d}(X), \ldots, \sigma_{d,d}(X))$.

On a d'abord la formule suivante, qui donne une expression plus explicite pour ces polynômes :

PROPOSITION 3.2. *On fait la convention que $Y_0 = 1$. Soit Σ_j l'ensemble des racines primitives j-ièmes de l'unité. On a alors*

$$Q_{j,d}(Y) = (-1)^{d\varphi(j)} \prod_{\zeta \in \Sigma_j} \Big(\sum_{l=0}^{d} (-1)^l \zeta^{d-l} Y_l \Big).$$

Démonstration. Soit $P(T) = \prod_{k=1}^{d} (T - X_k)$. On a

$$P(T) = \sum_{l=0}^{d} (-1)^l \sigma_{l,d}(X) T^{d-l},$$

avec la convention que $\sigma_{0,d}(X) = 1$.

D'autre part, $\phi_j(T) = \prod_{\zeta \in \Sigma_j} (T - \zeta)$. Donc comme on a $T_{j,d}(X) = \prod_{k=1}^{d} \phi_j(X_k)$, il vient

$$\begin{aligned} T_{j,d}(X) &= (-1)^{d\varphi(j)} \prod_{\zeta \in \Sigma_j} \prod_{k=1}^{d} (\zeta - X_k) \\ &= (-1)^{d\varphi(j)} \prod_{\zeta \in \Sigma_j} \Big(\sum_{l=0}^{d} (-1)^l \zeta^{d-l} \sigma_{l,d}(X) \Big) \end{aligned}$$

et il suffit de remplacer $\sigma_{l,d}(X)$ par Y_l pour terminer la démonstration. ∎

PROPOSITION 3.3. *Soit $d \geq 1$. Les polynômes $T_{1,d}(X), \ldots, T_{d,d}(X)$ sont algébriquement indépendants sur $\mathbb{C}$, et il en est de même pour les polynômes $Q_{1,d}, \ldots, Q_{d,d}$.*

Démonstration. Nous allons raisonner par récurrence sur l'entier d. Pour $d = 1$, on a $T_{1,1}(X_1) = \sigma_{1,1}(X_1) = X_1$, de sorte que le résultat est trivial. Ceci se produit aussi pour $d = 2$, puisque $T_{1,2}(X_1, X_2) = \sigma_{2,2}(X_1, X_2) - \sigma_{1,2}(X_1, X_2) + 1$ et $T_{2,2}(X_1, X_2) = \sigma_{2,2}(X_1, X_2) + \sigma_{1,2}(X_1, X_2) + 1$.

Nous supposons maintenant le résultat acquis pour $d-1$ variables, et nous démontrons l'assertion pour d. On raisonne par l'absurde. On suppose qu'il existe un polynôme P à coefficients dans $\mathbb{C}$, non nul, en d variables $Y_1, \ldots, Y_d$, tel que $P(T_{1,d}(X), \ldots, T_{d,d}(X)) = 0$. On peut clairement choisir P de degré minimal possible en Y_d, et on a alors $Q(Y_1, \ldots, Y_{d-1}) = P(Y_1, \ldots, Y_{d-1}, 0)$, qui est un polynôme non nul.

Choisissons λ racine primitive d-ième de 1. On note que $b_j = \phi_j(\lambda) \neq 0$ pour $j \leq d-1$, et que l'on a

$$T_{j,d}(X_1, \ldots, X_{d-1}, \lambda) = \Big(\prod_{k=1}^{d-1} \phi_j(X_k) \Big) \phi_j(\lambda) = b_j T_{j,d-1}(X_1, \ldots, X_{d-1}).$$

Par contre, si $j = d$, on a $T_{d,d}(X_1, \ldots, X_{d-1}, \lambda) = 0$. Il en résulte que

$$0 = P(b_1 T_{1,d-1}(X_1, \ldots, X_{d-1}), \ldots, b_{d-1} T_{d-1,d-1}(X_1, \ldots, X_{d-1}), 0)$$

est égal à

$$Q(b_1 T_{1,d-1}(X_1,\dots,X_{d-1}),\dots,b_{d-1}T_{d-1,d-1}(X_1,\dots,X_{d-1}))=0,$$

ce qui est absurde puisque par l'hypothèse de récurrence, les $T_{j,d-1}$ sont algébriquement indépendants et Q est non nul. Ceci démontre l'assertion.

La dernière affirmation vient du fait que les $\sigma_{k,d}(X)$ sont algébriquement indépendants. ∎

Nous allons maintenant appliquer les résultats de A. Płoski à la famille des polynômes $Q_{1,d},\dots,Q_{d+1,d}$. On a le résultat suivant :

PROPOSITION 3.4. *Soit μ_d le degré de l'extension $\mathbb{C}(Q_{1,d},\dots,Q_{d+1,d})\subset\mathbb{C}(Y_1,\dots,Y_d)$. Si P_d est l'un des polynômes de degré minimal, défini à une constante multiplicative non nulle près telle que $P(Q_{1,d},\dots,Q_{d+1,d})=0$, alors on a*

$$\mu_d \deg(P_d)=\varphi(1)\cdots\varphi(d+1).$$

Démonstration. Le fait que les polynômes $Q_{j,d}$, $1\le j\le d$, soient algébriquement indépendants est une conséquence de la proposition 3.3. La famille $\{Q_{1,d},\dots,Q_{d+1,d}\}$ considérée est donc non dégénérée.

Le degré de $Q_{j,d}$ est clairement $\varphi(j)$. Par suite, $Q_{1,d}$ et $Q_{2,d}$ sont deux polynômes de plus bas degré parmi les $\mathbb{Q}_{j,d}$.

La famille $Q^+_{j,d}$, $2\le j\le d+1$, est telle que le système d'équations $Q^+_{j,d}=0$ n'a comme solution que l'élément nul de $\mathbb{C}^d$. En effet, il résulte immédiatement des formules donnant les $Q_{j,d}$ que

$$Q^+_{j,d}(Y)=(-1)^{d\varphi(j)}\prod_{\zeta\in\Sigma_j}\Big(\sum_{l=1}^{d}(-1)^l\zeta^{d-l}Y_l\Big).$$

Soit $y=(y_1,\dots,y_d)$ une solution du système d'équations $Q^+_{j,d}=0$, $j=2,\dots,d+1$. On voit donc que pour tout j, il existe une racine primitive j-ième de l'unité ζ_j telle que $\sum_{l=1}^{d}(-1)^l\zeta_j^{d-l}y_l=0$.

Il existe $x\in\mathbb{C}^d$ tel que $y_i=\sigma_{i,d}(x)$ pour $i=1,\dots,d$. Il existe donc pour tout j une racine primitive de l'unité ζ_j telle que $\sum_{l=1}^{d}(-1)^l\zeta_j^{d-l}\sigma_{l,d}(x)=0$. Mais l'expression $\sum_{l=1}^{d}(-1)^l\zeta_j^{d-l}\sigma_{l,d}(x)$ est égale à $\prod_{k=1}^{d}(\zeta_j-x_k)-\zeta_j^d$. Le polynôme $H(T)=\prod_{k=1}^{d}(T-x_k)-T^d$, qui est de degré $\le d-1$, admet donc les d racines distinctes ζ_j, $j=2,\dots,d+1$, et par suite est identiquement nul. Ceci fournit que $y_l=\sigma_{l,d}(x)$ est nul pour tout l, ce qui démontre l'assertion.

La quantité $\max_{1\le j\le n+1}\{\prod_{i\ne j}\deg(Q_{i,d})\}$ est égale à $\varphi(1)\cdots\varphi(d+1)$.

Le théorème 3.1 donne alors que

$$\deg(P_d^{\mu_d})=\mu_d\deg(P_d)=\varphi(1)\cdots\varphi(d+1).\ \blacksquare$$

4. Propriétés du polynôme P_d. Pour $d = 2$, des calculs donnent

$$P_2(Z_1, Z_2, Z_3) = 4Z_3 - Z_1^2 - 3Z_2^2 + 6Z_1 + 6Z_2 - 12.$$

Ce polynôme est de degré 2, égal à $\varphi(1)\varphi(2)\varphi(3)$. D'autre part, si on a t_1, t_2, t_3 et θ non nuls dans $\mathbb{C}$ tels que $P_2(t_1Z_1, t_2Z_2, t_3Z_3) = \theta P_2(Z_1, Z_2, Z_3)$, on voit immédiatement que $t_1 = t_2 = t_3 = \theta = 1$.

Cette partie est consacrée à la démonstration du résultat suivant, qui généralise ce qui précède à $d \geq 2$ quelconque :

PROPOSITION 4.1. *Soit, pour $d \geq 2$, $P_d(Y_1, \ldots, Y_{d+1})$ le polynôme non nul à $d+1$ variables, défini à une constante multiplicative non nulle près, irréductible, tel que $P_d(Q_{1,d}, \ldots, Q_{d+1,d}) = 0$. On a alors :*

(i) *Le degré de P_d est égal à $\varphi(1) \cdots \varphi(d+1)$.*

(ii) *Si $t = (t_1, \ldots, t_{d+1}) \in (\mathbb{C}^*)^{d+1}$ est tel qu'il existe une constante $\theta \neq 0$ dans $\mathbb{C}$ telle que*

$$P_d(t_1Z_1, \ldots, t_{d+1}Z_{d+1}) = \theta P_d(Z_1, \ldots, Z_{d+1})$$

alors $t_j = 1$ pour $1 \leq j \leq d+1$, et $\theta = 1$.

Démonstration. Nous allons démontrer ce résultat par récurrence sur l'entier d. Il résulte de ce qui précède que le résultat est vrai si $d = 2$. On va montrer que si le résultat est vrai pour $d-1$, il est vrai pour d.

4.1. *Démonstration de* (i) *pour d.* Le polynôme $P_d(Z_1, \ldots, Z_d, 0)$ est non nul, par l'hypothèse d'irréductibilité faite sur ce polynôme. D'autre part, par définition du polynôme P_d, si on y remplace Y_j par $\sigma_{j,d}(X)$, on trouve que $P_d(T_{1,d}(X), \ldots, T_{d+1,d}(X)) = 0$. On remplace la variable X_d par une racine primitive $(d+1)$-ième de l'unité ζ. On a alors $T_{j,d}(X_1, \ldots, X_{d-1}, \zeta) = \phi_j(\zeta)T_{j,d-1}(X)$, où $X = (X_1, \ldots, X_{d-1})$, pour $1 \leq j \leq d$, le terme $T_{d+1,d}$ donnant 0. Par suite, $P_d(\phi_1(\zeta)T_{1,d-1}(X), \ldots, \phi_d(\zeta)T_{d,d-1}(X), 0) = 0$. Le polynôme $P_{d-1}(Z_1, \ldots, Z_d)$ divise alors $P_d(\phi_1(\zeta)Z_1, \ldots, \phi_d(\zeta)Z_d, 0)$. Par conséquent, le polynôme

$$H_\zeta = P_{d-1}\left(\frac{Z_1}{\phi_1(\zeta)}, \ldots, \frac{Z_d}{\phi_d(\zeta)}\right)$$

divise $P_d(Z_1, \ldots, Z_d, 0)$. Par la partie (ii) de l'hypothèse de récurrence, pour des ζ distincts dans l'ensemble Σ_{d+1} des racines primitives de l'unité, les polynômes irréductibles H_ζ ne sont pas égaux à une constante multiplicative près, puisque $\phi_1(\zeta) \neq \phi_1(\lambda)$ si $\zeta \neq \lambda$. Donc le produit $\prod_{\zeta \in \Sigma_{d+1}} H_\zeta$ divise $P_d(Z_1, \ldots, Z_d, 0)$.

Par la proposition 3.4, P_d est toujours de degré $\leq \varphi(1) \cdots \varphi(d+1)$, donc ce sera aussi le cas pour $P_d(Z_1, \ldots, Z_d, 0)$. Comme par la partie (i) de l'hypothèse de récurrence, le degré de P_{d-1} est $\varphi(1) \cdots \varphi(d)$, le degré du produit $\prod_{\zeta \in \Sigma_{d+1}} H_\zeta$ est $\varphi(1) \cdots \varphi(d+1)$. Il en résulte que le degré de

$P_d(Z_1,\dots,Z_d,0)$ est égal à $\varphi(1)\cdots\varphi(d+1)$, et que de plus il existe une constante τ non nulle telle que

$$\tau \prod_{\zeta\in\Sigma_{d+1}} P_{d-1}\left(\frac{Z_1}{\phi_1(\zeta)},\dots,\frac{Z_d}{\phi_d(\zeta)}\right) = P_d(Z_1,\dots,Z_d,0). \tag{2}$$

Comme le degré de P_d est plus grand que le degré de $P_d(Z_1,\dots,Z_d,0)$, et au plus égal à $\varphi(1)\cdots\varphi(d+1)$, il est égal à cette quantité, ce qui démontre l'assertion (i) pour d.

4.2. *Démonstration de* (ii) *pour* d. Soient $t=(t_1,\dots,t_{d+1})\in(\mathbb{C}^*)^{d+1}$ et $\theta\in\mathbb{C}^*$ tels que $P_d(t_1Z_1,\dots,t_{d+1}Z_{d+1})=\theta P_d(Z_1,\dots,Z_{d+1})$.

On commence par faire $Z_{d+1}=0$, d'où

$$P_d(t_1Z_1,\dots,t_dZ_d,0)=\theta P_d(Z_1,\dots,Z_d,0).$$

Nous allons utiliser la formule (2). Il vient, après simplification par τ,

$$\prod_{\zeta\in\Sigma_{d+1}} P_{d-1}\left(\frac{t_1Z_1}{\phi_1(\zeta)},\dots,\frac{t_dZ_d}{\phi_d(\zeta)}\right)=\theta\prod_{\zeta\in\Sigma_{d+1}} P_{d-1}\left(\frac{Z_1}{\phi_1(\zeta)},\dots,\frac{Z_d}{\phi_d(\zeta)}\right).$$

Soit $\zeta\in\Sigma_{d+1}$. Il résulte de la formule précédente qu'il existe $\zeta^*\in\Sigma_{d+1}$ tel que $P_{d-1}(t_1Z_1/\phi_1(\zeta),\dots,t_dZ_d/\phi_d(\zeta))$ et $P_{d-1}(Z_1/\phi_1(\zeta^*),\dots,Z_d/\phi_d(\zeta^*))$ diffèrent d'une constante multiplicative non nulle. Si on remplace $Z_j/\phi_j(\zeta^*)$ par Y_j, la partie (ii) de l'hypothèse de récurrence implique que pour tout j, on a $\phi_j(\zeta^*)=\tau_j\phi_j(\zeta)$, où on a noté $\tau_j=t_j^{-1}$. Soit Ω_{d+1} l'ensemble des d-uplets d'éléments de $\mathbb{C}^*$ de la forme $(\phi_1(\zeta),\dots,\phi_d(\zeta))$, où $\zeta\in\Sigma_{d+1}$. Alors Ω_{d+1} est un ensemble fini à $\varphi(d+1)$ éléments, et l'application $x=(x_1,\dots,x_d)\in\Omega_{d+1}\mapsto(\tau_1x_1,\dots,\tau_dx_d)$ applique Ω_{d+1} dans Ω_{d+1}. Comme elle est clairement injective, c'est donc une permutation de l'ensemble Ω_{d+1}. Il en résulte immédiatement que tous les τ_j sont des racines de l'unité.

Comme $2\le d$, on peut reprendre l'égalité $\phi_2(\zeta^*)=\tau_2\phi_2(\zeta)$, qui s'écrit $\zeta^*+1=\tau_2(\zeta+1)$. Si on prend le conjugué, il vient

$$\frac{\zeta^*+1}{\zeta^*}=\frac{\zeta+1}{\tau_2\zeta},$$

d'où $\zeta^*=\zeta\tau_2^2$. En remplaçant dans la formule de départ, il vient que $\zeta\tau_2^2+1=\tau_2(\zeta+1)$, d'où $\tau_2=1$ ou $\tau_2=\zeta^{-1}$.

Si $\tau_2\ne1$, on a $\tau_2=\zeta^{-1}$, donc τ_2 est une racine de l'unité d'ordre $d+1$ exactement. Si on prend un élément quelconque $\omega=(\omega_1,\dots,\omega_d)$ de Ω_{d+1} (donc $\omega_j\ne0$ pour tout j), il en résulte que les $(\tau_1^l\omega_1,\dots,\tau_d^l\omega_d)\in\Omega_{d+1}$ sont tous distincts pour $l=0,\dots,d$, car si deux d'entre eux sont égaux, on a $\tau_2^l\omega_2=\tau_2^k\omega_2$ par exemple pour $l>k$, donc $\tau_2^{l-k}=1$, ce qui, puisque $0<l-k\le d$, contredit le fait que τ_2 est une racine primitive $(d+1)$-ième de 1. Mais comme le cardinal de Ω_{d+1} est $\varphi(d+1)<d+1$, on a une contradiction.

Donc $\tau_2 = 1$, il en résulte immédiatement que $\zeta^* = \zeta$, et par suite $\tau_j = 1$ pour $j = 1, \ldots, d$. Donc les t_j, $j = 1, \ldots, d$, sont tous égaux à 1. Il nous reste à montrer que $\theta = 1$ et $t_{d+1} = 1$. On a

$$P_d(Z_1, \ldots, Z_d, t_{d+1}Z_{d+1}) = \theta P_d(Z_1, \ldots, Z_d, Z_{d+1}).$$

En faisant $Z_{d+1} = 0$, comme le polynôme $P_d(Z_1, \ldots, Z_d, 0)$ n'est pas nul, on trouve que $\theta = 1$. Écrivons

$$P_d(Z_1, \ldots, Z_d, Z_{d+1}) = \sum_{k=0}^{N} A_k(Z_1, \ldots, Z_d) Z_{d+1}^k$$

avec $A_N \neq 0$. L'égalité se traduit par le fait que si $A_k \neq 0$, on a $t_{d+1}^k = 1$. Donc t_{d+1} est une racine de l'unité. Soit m son ordre ; nous allons supposer $m \geq 2$, et montrer qu'il y a contradiction.

Les indices k tels que $A_k \neq 0$ sont tous multiples de m. Donc le polynôme P_d s'écrit

$$P_d(Z_1, \ldots, Z_{d+1}) = \sum_{j=0}^{M} A_{jm}(Z) Z_{d+1}^{jm}$$

où $mM = N$. Soit S_d le polynôme

$$S_d(Z_1, \ldots, Z_{d+1}) = \sum_{j=0}^{M} A_{jm}(Z) Z_{d+1}^{j}.$$

On a donc

$$P_d(Z_1, \ldots, Z_{d+1}) = S_d(Z_1, \ldots, Z_{d+1}^m)$$

et par définition de P_d,

$$S_d(T_{1,d}(X), \ldots, T_{d,d}(X), T_{d+1,d}(X)^m) = 0.$$

On dérive par rapport à la variable X_d ; il vient $0 = A + B$ avec

$$A = \sum_{j=1}^{d} \phi_j'(X_d) T_{j,d-1}(X) \frac{\partial S_d}{\partial Z_j}(T_{1,d}(X), \ldots, T_{d,d}(X), T_{d+1,d}(X)^m),$$

$$B = m\phi_{d+1}'(X_d)(\phi_{d+1}(X_d))^{m-1}(T_{d+1,d-1}(X))^m \times \frac{\partial S_d}{\partial Z_{d+1}}(T_{1,d}(X), \ldots, T_{d,d}(X), T_{d+1,d}(X)^m).$$

On remplace encore X_d par ζ, une racine primitive $(d+1)$-ième de 1, et parce que $m - 1 \geq 1$, il vient $(\phi_{d+1}(\zeta))^{m-1} = 0$, donc $B = 0$, et par suite

$$\sum_{j=1}^{d} \phi_j'(\zeta) T_{j,d-1}(X) \frac{\partial S_d}{\partial Z_j}(\phi_1(\zeta) T_{1,d-1}(X), \ldots, \phi_d(\zeta) T_{d,d-1}(X), 0) = 0,$$

ou encore, compte tenu du fait que $P_d(Z_1,\dots,Z_d,0) = S_d(Z_1,\dots,Z_d,0)$,

$$\sum_{j=1}^{d} \phi_j'(\zeta) T_{j,d-1}(X)\, \frac{\partial P_d}{\partial Z_j}(\phi_1(\zeta)T_{1,d-1}(X),\dots,\phi_d(\zeta)T_{d,d-1}(X),0) = 0.$$

Par suite, le polynôme

$$\sum_{j=1}^{d} \phi_j'(\zeta) Z_j\, \frac{\partial P_d}{\partial Z_j}(\phi_1(\zeta)Z_1,\dots,\phi_d(\zeta)Z_d,0)$$

est divisible par $P_{d-1}(Z_1,\dots,Z_d)$, ou encore, le polynôme

$$\sum_{j=1}^{d} \frac{\phi_j'(\zeta)}{\phi_j(\zeta)}\, Z_j\, \frac{\partial P_d}{\partial Z_j}(Z_1,\dots,Z_d,0)$$

est divisible par le polynôme $P_{d-1}(Z_1/\phi_1(\zeta),\dots,Z_d/\phi_d(\zeta))$.

Nous allons maintenant utiliser de nouveau la relation (2) que nous rappelons :

$$P_d(Z_1,\dots,Z_d,0) = \tau \prod_{\lambda\in\Sigma_{d+1}} P_{d-1}\Big(\frac{Z_1}{\phi_1(\lambda)},\dots,\frac{Z_d}{\phi_d(\lambda)}\Big).$$

La dérivée partielle de $P_d(Z_1,\dots,Z_d,0)$ par rapport à la variable Z_j est égale à

$$\tau \sum_{\eta\in\Sigma_{d+1}} \frac{1}{\phi_j(\eta)}\, \frac{\partial P_{d-1}}{\partial Z_j}\Big(\frac{Z_1}{\phi_1(\eta)},\dots,\frac{Z_d}{\phi_d(\eta)}\Big) \prod_{\lambda\neq\eta} P_{d-1}\Big(\frac{Z_1}{\phi_1(\lambda)},\dots,\frac{Z_d}{\phi_d(\lambda)}\Big).$$

Cette dernière quantité est congrue modulo $P_{d-1}(Z_1/\phi_1(\zeta),\dots,Z_d/\phi_d(\zeta))$ à

$$\tau\, \frac{1}{\phi_j(\zeta)}\, \frac{\partial P_{d-1}}{\partial Z_j}\Big(\frac{Z_1}{\phi_1(\zeta)},\dots,\frac{Z_d}{\phi_d(\zeta)}\Big) \prod_{\lambda\neq\zeta} P_{d-1}\Big(\frac{Z_1}{\phi_1(\lambda)},\dots,\frac{Z_d}{\phi_d(\lambda)}\Big).$$

Donc la quantité

$$\sum_{j=1}^{d} \frac{\phi_j'(\zeta)}{\phi_j(\zeta)}\, Z_j\, \frac{\partial P_d}{\partial Z_j}(Z_1,\dots,Z_d,0)$$

est congrue modulo $P_{d-1}(Z_1/\phi_1(\zeta),\dots,Z_d/\phi_d(\zeta))$ à

$$\Big[\tau \sum_{j=1}^{d} \frac{\phi_j'(\zeta)}{\phi_j(\zeta)^2}\, Z_j\, \frac{\partial P_{d-1}}{\partial Z_j}\Big(\frac{Z_1}{\phi_1(\zeta)},\dots,\frac{Z_d}{\phi_d(\zeta)}\Big)\Big] \prod_{\lambda\neq\zeta} P_{d-1}\Big(\frac{Z_1}{\phi_1(\lambda)},\dots,\frac{Z_d}{\phi_d(\lambda)}\Big).$$

Par suite,

$$\sum_{j=1}^{d} \frac{\phi_j'(\zeta)}{\phi_j(\zeta)^2}\, Z_j\, \frac{\partial P_{d-1}}{\partial Z_j}\Big(\frac{Z_1}{\phi_1(\zeta)},\dots,\frac{Z_d}{\phi_d(\zeta)}\Big)$$

est divisible par $P_{d-1}(Z_1/\phi_1(\zeta), \dots, Z_d/\phi_d(\zeta))$. Ceci veut dire encore que

$$\sum_{j=1}^{d} \frac{\phi_j'(\zeta)}{\phi_j(\zeta)} Z_j \frac{\partial P_{d-1}}{\partial Z_j}(Z_1, \dots, Z_d)$$

est divisible par $P_{d-1}(Z_1, \dots, Z_d)$. Pour des raisons de degré, il existe une constante $\tau(\zeta)$ telle que

$$\sum_{j=1}^{d} \frac{\phi_j'(\zeta)}{\phi_j(\zeta)} Z_j \frac{\partial P_{d-1}}{\partial Z_j}(Z_1, \dots, Z_d) = \tau(\zeta) P_{d-1}(Z_1, \dots, Z_d).$$

On écrit $P_{d-1}(Z) = \sum a_\nu Z^\nu$. La relation précédente donne que

$$\sum_{j=1}^{d} \nu_j \frac{\phi_j'(\zeta)}{\phi_j(\zeta)} = \tau(\zeta)$$

si $a_\nu \neq 0$. Comme $\phi_1'(\zeta)/\phi_1(\zeta) = 1/(\zeta - 1)$ est non nul, on a une relation non triviale entre les ν tels que a_ν soit non nul. Ceci donne une relation de la forme

$$c_1\nu_1 + \dots + c_d\nu_d = b,$$

avec cette fois-ci les c_j dans $\mathbb{Z}$ non tous nuls, b indépendant de ν, valide pour tous les d-uplets ν tels que a_ν soit non nul.

Posons $t_j = \exp(c_j)$. Par ce qui précède, l'un au moins des t_j n'est pas égal à 1. L'expression $P_{d-1}(t_1Z_1, \dots, t_dZ_d)$ est égale à

$$\sum a_\nu t_1^{\nu_1} \cdots t_d^{\nu_d} Z^\nu = \exp(b) \sum a_\nu Z^\nu = \exp(b) P_{d-1}(Z_1, \dots, Z_d),$$

ce qui contredit la partie (ii) de l'hypothèse de récurrence. Par suite, on ne peut avoir $m \geq 2$, donc l'ordre m de t_{d+1} est égal à 1, et $t_{d+1} = 1$, ce qui achève la démonstration de la proposition. ∎

5. Démonstration du théorème 1.3. On utilise le théorème 3.1. On a déjà vu que les hypothèses de ce théorème étaient satisfaites par $Q = (Q_{1,d}, \dots, Q_{d+1,d})$. Par la proposition 4.1, le degré du polynôme P_d, défini à une constante multiplicative non nulle près, liant algébriquement $Q_{1,d}, \dots, Q_{d+1,d}$ et de degré minimal pour cette propriété, est égal à $\varphi(1) \cdots$ $\cdots \varphi(d+1)$. Si μ_d est le degré de $\mathbb{C}(Y_1, \dots, Y_d)$ sur $\mathbb{C}(Q_{1,d}, \dots, Q_{d+1,d})$, la proposition 3.4 montre que l'on a la relation $\mu_d \deg(P_d) = \varphi(1) \cdots \varphi(d+1)$. Il en résulte que $\mu_d = 1$, de sorte que

$$\mathbb{C}(Y_1, \dots, Y_d) = \mathbb{C}(Q_{1,d}, \dots, Q_{d+1,d}).$$

En tenant compte du fait que $Q_{d+1,d}$ est algébrique sur $\mathbb{C}(Q_{1,d}, \dots, Q_{d,d})$, on peut donc exprimer chaque Y_j sous la forme

$$Y_j = \frac{U_j(Q_{1,d}, \dots, Q_{d+1,d})}{V_j(Q_{1,d}, \dots, Q_{d,d})},$$

où V_j est un polynôme non nul en d variables. Remplaçons les Y_j par les $\sigma_{j,d}(X)$; il vient que

$$\sigma_{j,d}(X) = \frac{U_j(T_{1,d}(X), \dots, T_{d+1,d}(X))}{V_j(T_{1,d}(X), \dots, T_{d,d}(X))}.$$

Soit U l'ouvert de Zariski de $\mathbb{C}^d$ défini par $\prod_{j=1}^{d} V_j(T_{1,d}(X), \dots, T_{d,d}(X)) \neq 0$. Soient $P(X) = \prod_{k=1}^{d}(X - x_k)$ et $Q(X) = \prod_{k=1}^{d}(X - y_k)$ deux polynômes tels que $x = (x_1, \dots, x_d)$ et $y = (y_1, \dots, y_d)$ soient dans U, tels qu'aucune des composantes x_k et y_k de x et y ne soit une racine de l'unité d'ordre $\leq d+1$, et tels que $r_n(P) = r_n(Q)$ si $1 \leq n \leq d+1$. Comme on l'a vu, la donnée des $r_n(P)$, $1 \leq n \leq d+1$, est alors équivalente à la donnée des $T_{j,d}(x)$, $1 \leq j \leq d+1$, et de même la donnée des $r_n(Q)$, $1 \leq n \leq d+1$, est équivalente à la donnée de $T_{j,d}(y)$, $1 \leq j \leq d+1$. Donc $T_{j,d}(x) = T_{j,d}(y)$ pour $1 \leq j \leq d+1$. Comme les $V_j(T_{1,d}(x), \dots, T_{d,d}(x))$ et les $V_j(T_{1,d}(y), \dots, T_{d,d}(y))$ sont non nuls, les égalités précédentes impliquent que $\sigma_{j,d}(x) = \sigma_{j,d}(y)$ pour $j = 1, \dots, d$, et par suite les polynômes $P(X)$ et $Q(X)$ sont égaux, ce qui termine la démonstration du théorème 1.3. ∎

Références

[1] D. Fried, *Cyclic resultants of reciprocal polynomials*, dans : Holomorphic Dynamics (Mexico, 1986), Lectures Notes in Math. 1345, Springer, 1988, 124–128.

[2] C. Hillar, *Cyclic resultants*, J. Symbolic Comput. 39 (2005), 653–669; erratum, ibid. 40 (2005), 1126–1127.

[3] C. Hillar and L. Levine, *Polynomial recurrences and cyclic resultants*, Proc. Amer. Math. Soc. 135 (2007), 1607–1618.

[4] A. Płoski, *Algebraic dependence and polynomial automorphisms*, Bull. Polish Acad. Sci. Math. 34 (1986), 653–659.

Département de Mathématiques et Mécanique
Laboratoire N. Oresme, Campus II
Université de Caen
Boulevard du Maréchal Juin
B.P. 5186
14032 Caen Cedex, France
E-mail: bezivin@math.unicaen.fr
http://www.math.unicaen.fr/~bezivin

Reçu le 28.5.2007 (5450)